ANALYSIS

PC running slowly? You may be a node in a vast cryptomining network

BY PAUL GILLIN
(HTTPS://SILICONANGLE.COM/BLOG/AUTHOR/PAULGILLIN/)

UPDATED 17:36 EST . 02 FEBRUARY 2018

That open tab in the background of the browser you're looking at right now could be slowing your computer to a crawl. If you're reading on a smartphone, it could even fry your device.

Cryptomining

(https://siliconangle.com/blog/2017/10/15/cryptomining-goes-mainstream-hundreds-millions-users-targeted-hijacking-scripts/) is the hottest thing in cybercrime right now, and many victims don't even know they've been affected. Cryptomining software hijacks personal computers and mobile devices and turns them into nodes on large networks that create cryptocurrencies. "Mining" in this context means validating transactions by solving mathematical problems. Each successful solution generates a small amount of income for the miner in the form of one of the more than 1,500 cryptocurrencies (https://coinmarketcap.com/all/views/all/) that are on the market.

“It’s extremely hard to detect,” said Alex Vaystikh, chief technology officer at SecBI Ltd., which makes a cyber threat detection and network traffic analysis platform. “It’s basically a denial-of-service attack against your CPU.”

Attackers can avoid the often substantial cost of the hardware needed for mining by hijacking other people’s computers and diverting part of their processing speed to the task. The more compromised systems they can lash together, the bigger their return. One cryptomining operation that was uncovered last week affected an estimated 30 million computers (http://securityaffairs.co/wordpress/68258/malware/monero-mining-operation.html) .

What makes this new form of attack different from those that preceded it is that developers have figured out ways to hijack client machines from within a browser window. “It doesn’t actually require an infection, which is a lot more sinister that malware, in a way, because anybody can mine for coins,” said Jérôme Segura, lead malware intelligence analyst at Malwarebytes Inc.

Malware in the browser

Thieves are taking advantage of the fact that browsers have gotten a lot more capable in recent years. Every browser can run JavaScript programs, and most also support Web Assembly (http://webassembly.org/) , a component of the HTML5 standard that enables complex browser-based applications to run nearly as fast as they would natively on a desktop.

The rewards are so attractive — and the risks so small — that Malwarebytes recently reported (https://siliconangle.com/blog/2018/01/25/ransomware-attacks-decline-cybercriminals-turn-attention-cryptomining/) that cryptomining is on track to surpass the data-encrypting ransomware as the fastest-growing form of malware. “It’s a more sensible and straightforward way to make money without the trouble of encrypting files,” said. “You don’t need to bypass detection, and if you stay for 10 minutes you can generate 10 cents.”

How lucrative is it? Cisco Systems Inc.’s Talos security unit this week estimated (https://blog.talosintelligence.com/2018/01/malicious-xmr-mining.html) that a miner who can rope together just 2,000 PCs can generate $500 a day worth of cryptocurrency, or $182,500 per year. Botnets with a few million compromised systems “could be leveraged to generate more than $100 million per year,” Talos researchers wrote.

How it works

Cryptomining software is delivered in two basic forms. One is as conventional malware, which is spread through email attachments, or by a user clicking on a malicious link. Malware has a signature, so it can be caught by antivirus software.

The browser-based versions are more insidious. Website operators need embed only a small amount of JavaScript code to connect visitors to a cryptomining network such as Coinhive (https://coinhive.com/) , which advertises its service as a way for website operators to improve visitor engagement and deliver better services by earning money from cryptomining rather than advertising. Coinhive steals a percentage of each connected processor and adds it to a giant distributed processing network.

A second, more sophisticated approach uses Web Assembly to deliver compiled software modules to the browser. That code runs faster and thus generates bigger returns for miners.

Cryptomining software works on any browser and can hijack any processor. That means miners can potentially co-opt anything with a processor, from simple Raspberry Pi devices to smart exercise equipment. “We expect smart TVs and USB devices will soon come pre-infected,” said SecBI’s Vaystikh.

Miners favor Monero (https://getmonero.org/) , a type of currency that is considered highly secure and untraceable. “It’s anonymous, and criminals appreciate that,” Segura said. Another advantage of Monero is that it’s designed to be mined on a network of off-the-shelf processors. In contrast, bitcoin has become such a big business that expensive server farms are the only practical way to mine it.

Technically legal

There’s nothing illegal about cryptomining when the practice is disclosed. Where things get fuzzy is when website owners don’t tell their visitors that their devices have been hijacked. But those website owners themselves may not even know. “We’ve started seeing waves of legitimate websites and WordPress blogs getting hacked and injected with the mining scripts,” Segura said. YouTube was recently caught (https://arstechnica.com/information-technology/2018/01/now-even-youtube-serves-ads-with-cpu-draining-cryptocurrency-miners/) serving up cryptomining code via advertisements that had been legitimately purchased on Google’s DoubleClick ad network.

It’s nearly impossible for antimalware software to detect browser-based cryptomining software. About the only way to tell that a computer has been compromised is to monitor for network requests to JavaScript mining services. At one point last year, Malwarebytes was blocking 8

million requests a day to Coinhive.com, but “today there are a lot of copycats and other services using various proxies that make it much harder to block,” Segura said. “We don’t have as good an idea of the impact of cryptomining as we used to.”

The best way to tell if your computer has been hijacked is to watch for sudden and dramatic slowdowns in performance. Check the Task Manager on Windows or Activity Monitor on Macintosh to see if your browser is the culprit. If closing browser tabs restores normal performance, then a cryptominer is probably the culprit.

If there’s a silver lining, it’s that the only thing cryptomining software steals from its victims is processing power. However, that can add up to frustration and a significant impact on productivity across a large network of PCs inside a company. Also, though running CPUs at 100 percent won’t damage PCs, it can potentially overheat and destroy mobile devices.

Image: Wikimedia Commons (http://wellcomeimages.org/indexplus/obf_images/a0/b8/6bdc1586b4ef24e650b6b796777c.jpg)

LATEST STORIES from SiliconANGLE ®

Cryptocurrency investor sees gold in the tokenized infrastructure (https://siliconangle.com/blog/2018/03/02/crypto-investor-sees-gold-in-the-tokenized-infrastructure-polycon18/)

Ethereum's smart contacts give developers their day in the sun (https://siliconangle.com/blog/2018/03/02/ethereums-smart-contacts-give-developers-their-day-in-the-sun-polycon18/)

Amazon cloud power outage temporarily knocks out more than 240 online services (https://siliconangle.com/blog/2018/03/02/amazon-cloud-outage-knocks-240-online-services/)

While blockchain developers get paid, some legacy tech companies may be missing the boat (https://siliconangle.com/blog/2018/03/02/blockchain-developers-get-paid-legacy-tech-companies-may-missing-boat-polycon18/)

Beyond the AI hype: Experts weigh in on AI growing pains, modern use cases (https://siliconangle.com/blog/2018/03/02/beyond-ai-hype-experts-weigh-ai-growing-pains-modern-use-cases-ibmml/)

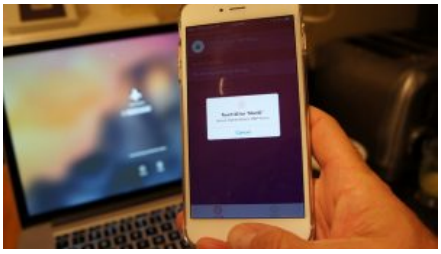
Microsoft bolsters Azure cloud’s computer vision and search capabilities (https://siliconangle.com/blog/2018/03/02/microsoft-bolsters-azures-computer-vision-search-capabilities/)

RELATED ARTICLES

Rakuten plans to build blockchain-based loyalty system with ‘borderless currency’

(https://siliconangle.com/blog/2018/02/27/rakuten-plans-build-blockchain-based-loyalty-system-borderless-currency/)

EMERGING TECH - BY KYT DOTSON (https://siliconangle.com/blog/author/kitdotson/) . 5 DAYS AGO



Israeli security firm Cellebrite claims to be able to hack iOS 11

(https://siliconangle.com/blog/2018/02/26/israeli-security-firm-cellebrite-claims-able-hack-ios-11/)

INFRASTRUCTURE - BY DUCAN RILEY (https://siliconangle.com/blog/author/duncanriley/) . 6 DAY…

Circle snaps up cryptocurrency exchange Poloniex in $400M deal

(https://siliconangle.com/blog/2018/02/26/circle-snaps-crypto-exchange-poloniex-rumored-400m-deal/)

EMERGING TECH - BY DUNCAN RILEY (https://siliconangle.com/blog/author/duncanriley/) . 6 DAYS…

Cybersecurity firm PhishMe acquired at $400M valuation, rebrands as Cofense

(https://siliconangle.com/blog/2018/02/26/cybersecurity-firm-phishme-acquired-400m-valuation-rebrands-cofense/)

INFRASTRUCTURE - BY ERIC DAVID (https://siliconangle.com/blog/author/ericdavid/) . 6 DAYS AGO

Security an enabler for government adoption of AWS cloud

(https://siliconangle.com/blog/2018/02/22/security-enabler-government-adoption-aws-cloud-thecube-awspublicsector/)

CLOUD - BY MARK ALBERTSON (https://siliconangle.com/blog/author/markalbertson/) . 1 WEEK AGO

AI tech combats cyberattack, cryptojacking

(https://siliconangle.com/blog/2018/02/22/ai-tech-combats-cyberattack-cryptojacking-thecube-cubeconversations/)

NEWS - BY MARK ALBERTSON (https://siliconangle.com/blog/author/markalbertson/) . 1 WEEK AGO

Arm unveils plans to use SIM cards to secure the 'internet of things'

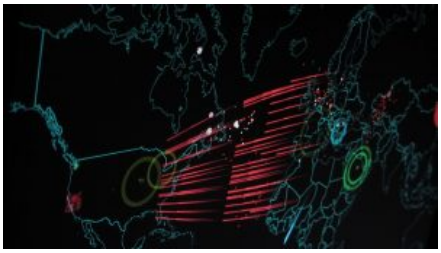
(https://siliconangle.com/blog/2018/02/21/arm-unveils-plans-use-sim-cards-secure-internet-things/)

INFRASTRUCTURE - BY MIKE WHEATLEY (https://siliconangle.com/blog/author/mikewheatley/) . 2…

McAfee: Cybercrime now costs the global economy $600B

(https://siliconangle.com/blog/2018/02/21/mcafee-report-claims-cybercrime-now-costs-global-economy-600b/)

INFRASTRUCTURE - BY DUNCAN RILEY (https://siliconangle.com/blog/author/duncanriley/) . 2…



Trillions of botnet requests drive massive rise in malicious login attempts

(https://siliconangle.com/blog/2018/02/20/trillions-botnet-requests-drive-massive-rise-malicious-login-attempts/)

INFRASTRUCTURE - BY DUNCAN RILEY (https://siliconangle.com/blog/author/duncanriley/) . 2…

CUBE EVENT COVERAGE

Check out more cube videos and stories (https://siliconangle.com/blog/category/cube-event-coverage/)

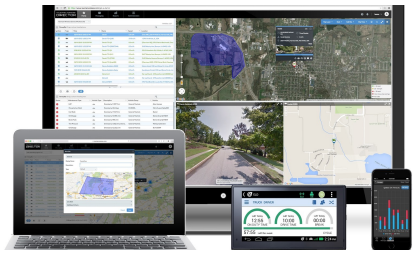
VOICE OF THE COMMUNITY (https://siliconangle.com?s_name=voice%20of%20community&cat_in=sponsor-posts&tag_in)

Analytics feeds machine maker’s global ambitions

(https://siliconangle.com/blog/2017/11/09/analytics-feeds-machine-makers-global-ambitions/)

Modern infrastructure management: accelerating productivity through machine learning

(https://siliconangle.com/blog/2017/10/20/modern-infrastructure-management-accelerating-productivity-machine-learning/)



Fleet analytics provider spins vehicle sensor data into productivity gold

(https://siliconangle.com/blog/2017/10/20/fleet-analytics-provider-spins-vehicle-sensor-data-productivity-gold/)

Big data leads a transformation in PC gaming

(https://siliconangle.com/blog/2017/10/13/big-data-leads-transformation-pc-gaming/)

UPCOMING CUBE EVENTS (https://www.thecube.net/upcomingevents/)

(https://www.thecube.net/dnc-2018)

RSA Conference USA 2018

(https://www.thecube.net/rsa-conference-usa-2018)

PBWC: Professional Business Women of California 2018

(https://www.thecube.net/pbwc-2018)

Dell Technologies World 2018

(https://www.thecube.net/dell-tech-world-2018)

KubeCon Europe 2018

(https://www.thecube.net/kubecon-eu-2018)

ServiceNow Knowledge 2018

(https://www.thecube.net/knowledge-2018)

Nutanix .NEXT New Orleans 2018

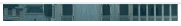
(https://www.thecube.net/next-no-2018)

Red Hat Summit 2018

(https://www.thecube.net/red-hat-summit-2018)

VeeamON 2018

(https://www.thecube.net/veeamon-2018)



Informatica World 2018

Join Our Community

For personalised content stay with us.

I AM INTERESTED IN

Please enter your email ID

SUBSCRIBE NOW

Cookies

We employ the use of cookies. Find out more. (https://siliconangle.com/terms-of-use/)

GOT IT!

(https://siliconangle.com)